We claim:

1. For an electronic signature device comprising a processor, a memory, a user input device including a first signature input device, and a device interface, all communicatively connected by at least one bus, a method of personalizing the electronic signature device to a user, comprising:

receiving a digitized written user signature of the user via the first signature input device;

generating a prime parameter, a sub-prime parameter, and a base parameter;

generating a signing private key;

generating a signing public key based on said prime, sub-prime, and base parameters;

generating a user public key based on said user private key and said prime and base parameters;

generating a biometric electronic template based on said digitized written user signature; and

storing said prime, sub-prime, and base parameters, said user private and public keys, and said biometric electronic template in the memory.

2. The method of claim 1, wherein said prime, sub-prime, and base parameters are based on Diffie-Hellman parameters.

3. The method of claim 1, wherein said prime, sub-prime, and base parameters are generated based on a seed value.

4. The method of claim 3, wherein the seed value is one of a random value and a pseudorandom number.

5. The method of claim 3, wherein the seed value is received from the user via the user interface.

6. The method of claim 1, wherein the user interface further comprises a password input device, and said method further comprises:

receiving a user password via the password input device;

generating a password encryption key based on the user password;

encrypting a known value with the password encryption key to produce an encrypted output; and

storing the encrypted known value in the memory.

7. The method of claim 6, wherein said known value is said biometrics electronic template.

8. The method of claim 1, wherein receiving said digitized user signature is repeated at least once.

9. The method of claim 1, wherein receiving said digitized user signature and generating said biometrics electronic template are repeated at least once.

10. The method of claim 1, wherein said biometric electronic template is generated based on a mathematic transformation of said digitized written user signature.

11. The method of claim 10, wherein the mathematical transformation is a Fourier transformation.

12. The method of claim 1, wherein the electronic signature device is communicatively connected to a certificate authority via the device interface, and said method further comprises:

sending a certificate request to the certificate authority;

receiving a certificate package from the certificate authority; and

storing said certificate package in the memory.

13. The method of claim 12, wherein said certificate request comprises said user public key.

14. The method of claim 13, wherein said certificate request further comprises at least one of said prime, sub-prime, and base parameters.

15. The method of claim 12, wherein said certificate request comprises said user public key and said prime parameter.

16. The method of claim 12, wherein said certificate package comprises a digital certificate.

17. The method of claim 12, wherein said certificate package comprises a digital certificate and a root value.

18. The method of claim 1, wherein the device interface is a card interface.

19. The method of claim 1, wherein the electronic signature device further comprises a power source that is at least one of a battery and the computer interface.

20. The method of claim 1, wherein the first signature input device is integral with the electronic signature device.

21. The method of claim 1, wherein the first signature input device is connected to the at least one bus through the device interface.

22. The method of claim 1, wherein at least a portion of said user interface is integral with the electronic signature device.

23. The method of claim 1, wherein at least a portion of said user interface is connected to the at least one bus through the device interface.

24. The method of claim 1, wherein said user public key is one of a random number and a pseudorandom number.

25. The method of claim 24, wherein said user public key is smaller than said sub-prime parameter.

26. For an electronic signature device comprising a processor, a memory having a biometric electronic template, a prime parameter, a sub-prime parameter, and a base parameter, user public data comprising a user public key, and a user private key stored therein, a user interface comprising a signature input device, a device interface adapted to interface a computer, and at least one bus operably connected to the processor, the memory, the user interface, and the device interface, a method of originating an electronically signed transaction, said method comprising:

verifying whether a user is permitted to originate the electronically signed transaction with the electronic signature device, comprising

receiving a digitized written originator signature via the user interface, and

comparing said digitized written originator signature against the biometric electronic template to produce a first verification result;

receiving a transaction package through one of the user interface and the device interface;

combining said transaction package and one of said digitized originator signature and a digitized user signature extracted from the biometric electronic template to produce an originator signature block;

generating an ephemeral private key based on the prime, sub-prime, and base parameters;

generating an ephemeral public key based on said ephemeral private key and the prime and base parameters;

generating a shared encryption key based on said ephemeral public key, the user public key, and the prime parameter;

encrypting said originator signature block with said shared encryption key to produce an encrypted signature block;

combining said encrypted signature block, said ephemeral private key, the prime parameter, and at least a portion of the user public data to produce an electronically signed transaction; and

if the user is verified, providing said electronically signed transaction via the device interface.

27. The method of claim 26, wherein the prime, sub-prime and base parameters are based on Diffie-Hellman parameters.

28. The method of claim 26, wherein the user interface further comprises a password input device, the memory has further stored therein an encrypted known value, and verifying whether the user is permitted to originate the electronically signed transaction with the electronic signature device further comprises

receiving a user password via the password input device;

generating a password encryption key based on the user password;

decrypting the encrypted known value with said password encryption key to produce a second verification result.

29. The method of claim 28, wherein the encrypted known value is the biometrics electronic template.

30. The method of claim 26, wherein receiving said digitized originator signature is repeated at least once.

31. The method of claim 26, wherein receiving said digitized originator signature and comparing said digitized written originator signature against the biometric electronic template to produce the first verification result are repeated at least once.

32. The method of claim 26, wherein comparing said digitized written originator signature against the biometric electronic template comprises

generating a temporary template based on said digitized written originator signature, and

comparing said temporary template to the biometric electronic template.

33. The method of claim 32, wherein said temporary template is generated based on a mathematic transformation of said digitized written originator signature.

34. The method of claim 33, wherein the mathematical transformation is a Fourier transformation.

35. The method of claim 26, wherein comparing said digitized written originator signature against the biometric electronic template comprises

generating a temporary signature based on the biometric electronic template, and

comparing said temporary signature to said digitized written originator signature.

36. The method of claim 35, wherein said temporary signature is generated based on a mathematic transformation of said digitized written originator signature.

37. The method of claim 36, wherein the mathematical transformation is a Fourier transformation.

38. The method of claim 26, wherein the at least a portion of the user public data comprises the user public key.